



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/498,716 | 02/07/2000 | Arjen K. Lenstra | 0225-4188 | 9213 |

7590 12/10/2003
Morgan & Finnegan, L.L.P.
345 Park Avenue
New York, NY 10154

EXAMINER

HENEGHAN, MATTHEW E

| | |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2134

DATE MAILED: 12/10/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/498,716

Applicant(s)

LENSTRA ET AL.

Examiner

Matthew Heneghan

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 February 2000 and 11 May 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 25-56 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 25-56 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 7 February 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 4,5,6,9,10. 6) ☐ Other: _____

DETAILED ACTION

1. Claims 25-56 have been examined. Claims 1-24 have been cancelled by a preliminary amendment.
2. Preliminary amendments to the instant application filed on 20 September 2000 and 11 May 2001 have been entered and are being considered in this first office action.

Information Disclosure Statement

3. The items in Information Disclosure Statements filed 2 March 2000, 28 August 2000, 1 September 2000, 30 January 2002, and 7 May 2002 have all been considered.
4. It is noted that the article "Doing More With Fewer Bits," by Brouwer et al., was submitted both in the IDS of 2 March 2000 and the IDS of 7 May 2002.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 25-56 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite in that they fail to point out what is included or excluded by the claim language.

Regarding claims 25, 33, 41, and 49, it is unclear as to how the limitations teach to the derivation of a public key.

As per claims 26-32, 34-40, 42-48, and 50-56, these claims are omnibus type claims. For purposes of the prior art search, these claims are being considered to only include the limitations of their respective parent claims, and thus stand or fall with them.

Regarding claims 32, 40, 48, and 56, the phrase "and related schemes" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention.

Regarding claim 37, it is unclear as to the meaning of "the public key."

Regarding claim 49, it is unclear to what application the claimed business has.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 25-56 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claimed matter solely teaches to the

mathematical manipulation of an abstract idea. There is no tangible output to the method.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 25-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over El Gamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory 31(4), 1985 in view of Brouwer et al., "Doing More With Fewer Bits," Advances in Cryptology - Asiacrypt '99, pp. 321-332 further in view of Lidl et al., "Introduction to Finite Fields and Their Applications," 1986, pp. 50-55.

El Gamal teaches a signature scheme based on discrete logarithms, and suggests that such a scheme can be extended from the $GF(p)$ to $GF(p^m)$. See part VI, "Conclusions and Remarks."

El Gamal does not disclose the conjugates and roots in such a case, or the order of the trace field employed.

Brouwer discloses a method using p^2-p+1 in $GF(p^6)$ (see section 3), and shows the derivation of the claimed roots (see section 3.3). The derivation of $F_g=X^3-BX^2+B^pX-1$ is a function of the polynomial and roots.

Lidl teaches that trace fields can be extended from one to the other over normal bases.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the scheme of El Gamal by using the roots disclosed by Brouwer, and extending them to $GF(p^2)$, using the method disclosed by Lidl.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

"Choosing Good Elliptic Curves," Author and Date Unknown, lists some algorithms for IEEE Standard P1363, including some pertinent trace field computations.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (703) 305-7727. The examiner can normally be reached on Monday-Thursday from 8:00 AM - 4:00 PM Eastern Time. The examiner can also be reached on alternate Fridays.

Art Unit: 2134

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, DC 20231

Or faxed to:

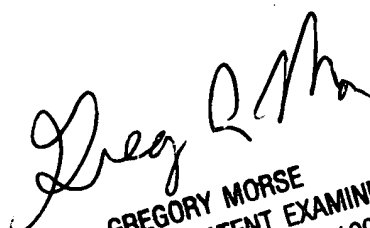
(703) 872-9306

Hand-delivered responses should be brought to Crystal Park 2, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

MEH

December 1, 2003


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100